This article originally appeared in the December 2020 School Business Affairs magazine and is reprinted with permission of the Association of School Business Officials International (ASBO). The text herein does not necessarily represent the views or policies of ASBO International, and use of this imprint does not imply any endorsement or recognition by ASBO International and its officers or affiliates.

Cybersecurity for School Districts: There's No Grading Curve

Is your district protected from cyber attacks? Now's the time for a preparedness assessment.

By Tim Rahschulte, PhD

BILLIONPHOTOS.COM/STOCK.ADOBE.COM

School is "back in session" this year like no prior year on record. School districts' preparations for an expertly crafted instructional plan for the new school year were overshadowed by the response (and defense) preparations necessary to address the spread of COVID-19.

As you and your fellow education leaders prepare for the winter break and reflect on the school year thus far, what grade do you think you deserve on your preparation efforts? How did you fare with social distancing? What about communications to your broad-based stakeholders? How were the adoption, integration, and effectiveness of new technologies, policies, and operational procedures? Did you earn an A? B+? D–?

Oh, and how did you do with addressing the onslaught of new cyber threats? The number of data breaches tripled last year, according to the K–12 Cybersecurity Resource Center, and this year we have been introduced to a new genre of attacks such as Zoom bombing, vishing (voice phishing), drive-by hacks,

cross-site scripting, eavesdropping, and more. Nearly 1,000 cybersecurity-related incidents have involved U.S. public schools since 2016, according to the K–12 Cybersecurity Resource Center—and that number reflects only the publicly reported cases.

What Now?

You managed through quite a bit this fall and likely deserve a winter respite. But alas, now is the time for spring preparations. Are you ready for what's next? The cycles can seem relentless because the landscape and environment are always changing, growing more complex by the year—check that, by the month. Hence, cyber readiness is never an absolute; it is either "no, but" or "yes, and" because there is always more to do. Consequently, preparedness is not graded on a curve. You don't get a pass based on effort; you earn preparedness grades based on outcomes.

Will data privacy and reputation for safety and security be more important in the spring? Yes. Will cyber risks and attacks increase in the spring? Yes.

The speed of technology evolution and associated cyber threats is hard to comprehend. We quickly moved from focusing on physical security and natural disaster preparedness and response readiness to addressing privacy threats to our compliance with the Health Insurance Portability and Accountability Act, the Family Educational Rights and Privacy Act, and the Children's Online Privacy Protection Act. We have become focused on networked devices and personal devices connected at work and at home and now, more than ever, on mobile applications and cloud-enabled solutions often described as the Internet of Things.

That just brings us up to current days, not the forecast of what's next.

Along the way, the need for a chief information security officer (or trust officer, privacy officer, or the like) arose. This critical position is charged with protecting data and business continuity and defending against what the National Institute of Standards and Technology refers to as the "World of Threats," which includes everything from natural disasters and pandemics to website defacement, denial-of-service attacks, data-scavenging attacks, wireless sniffers, unauthorized-user access, phishing, malware, eavesdropping, artificial intelligence–powered attacks, and, generally speaking, people.

Are You Paying Attention?

Just a few years ago, no one was forecasting 2019 to be the "Year of Ransomware," but that is exactly what the managing editors at *GovTech Magazine* labeled it. More than 140 local governments, police stations, and hospitals, and more than 100 schools and universities were victims of ransomware attacks.

Because of the level of disruption, four organizations—the Cybersecurity and Infrastructure Security Agency, the Multi-State Information Sharing and Analysis Center, the National Governors Association, and the National Association of State Chief Information Officers—came together in July 2019 and identified three critical recommendations regarding cybersecurity:

1. Back up your systems now and daily.
2. Reinforce cybersecurity awareness and education.
3. Revisit and refine cyber incident response plans.

With those three recommendations in mind, let's revisit the earlier questions: What grade did you earn this year? Are you ready for what's next? The three recommendations provide a great starting point if you know the priority of your systems, data segmentation, and backup (and perhaps more important, recovery) of data. Do you? Do you know the current state of readiness of your organizational culture?

People present a risk to cybersecurity, but they are also a perimeter for defense. Do you have playbooks and protocols in place (and practiced) for incident response?

Pop quiz: Your network administrator just notified you that a substitute teacher clicked a link from a school district laptop that is now displaying a text box saying that server access is halted until eight Bitcoins are paid to a specific account. What are your first three actions from your playbook?

Regardless of your readiness for this attack, your preparedness is never complete. One of the most effective points of preparedness is collaboration. Collaborate with your internal team, trusted advisers, and peers. Share your lessons learned, practices, protocols, and experiences. Doing so can extend your otherwise-limited and constrained resources.

One resource is the Cybersecurity Collaborative (www.cyberleadersunite.com), which shares its members' best practice assessments, policies, procedures, and other tools to help reduce cybercrime. Other resources include ASBO International's toolkit Working Together for Student Success: A Guide for SBOs and CTOs, available on the Global School Business Network, as well as resources from the ASBO member communities on the network.

Take a Readiness Assessment

Specific and relative to the three critical recommendations noted above, consider the following short yet powerful readiness assessment:

1. Full system inventory. A list of all assets and devices—including application programming interfaces, software programs, and other tools (local and in the cloud)—is available and regularly updated.

2. Backup and recovery system. All systems and data are cataloged and ranked using critical priority 1-2-3 criteria, and a full backup system is in place and tested regularly (along with recovery time).

3. Segmented network access. Critical data are segmented (separated) from single points of access so that if or when a breach occurs the data that are accessed are limited.

4. Detection systems. In addition to traditional firewalls, ransomware protection software and (early) detection system protocols are in place and tested regularly.

5. Trained workforce. Regular security awareness training (scheduled and "surprise" attacks) is mandatory and integrated into the business culture with a mind-set of "see something, say something."

6. Password security. A password management policy exists, is automated, and is enforced across the entire organization.

7. Viewable file extensions. All computers are configured to show file extensions (i.e., .doc) and therefore allow users to see a possible executable file (i.e., .exe) and reduce the chance of someone accidentally opening a malicious hacker file.

8. Email server controls. Beyond user-level controls, there are up-to-date antivirus controls and malware software protections on all email servers and (upstream) verified controls with the Internet service provider.

9. Managing plug-ins. All uses of Java and Flash (and other) plug-ins are known and managed with the most recent updates.

10. Limiting connectivity. The most critical data are kept on a private network, not connected to the Internet.

Your work is extremely hard; it also is extremely rewarding. The foundation of your success starts with the safety and security of all stakeholders. You won't be successful alone. Discuss these 10 assessment items with your cyber team, administrators, and others responsible for the safety and security of your district, employees, and customers. Rely on collaboration among your internal team, external peers, and partners to address the speed of the changing cybersecurity landscape.

Tim Rahschulte is chief executive officer of the Professional Development Academy and chief architect of the Enterprise Cybersecurity Leadership program. Email: timr@pdaleadership.com